Sécurisez votre ordinateur !

Benoit Mortgat

3 février 2005

1 Préambule

1.1 A propos de ce document

Ce document contient des images. N'hésitez pas à zoomer dessus, vous les verrez mieux. Toutefois, pour que ce document puisse être plus léger, leur qualité a été assez fortement dégradée. Ne vous en étonnez donc pas. Sans cela, ce document prendrait 3 fois plus de place.
Je vous conseille d'imprimer ce document. En effet, comme votre ordinateur sera amené à redémarrer, vous pourriez le perdre de vue.

1.2 Pourquoi sécuriser mon ordinateur ?

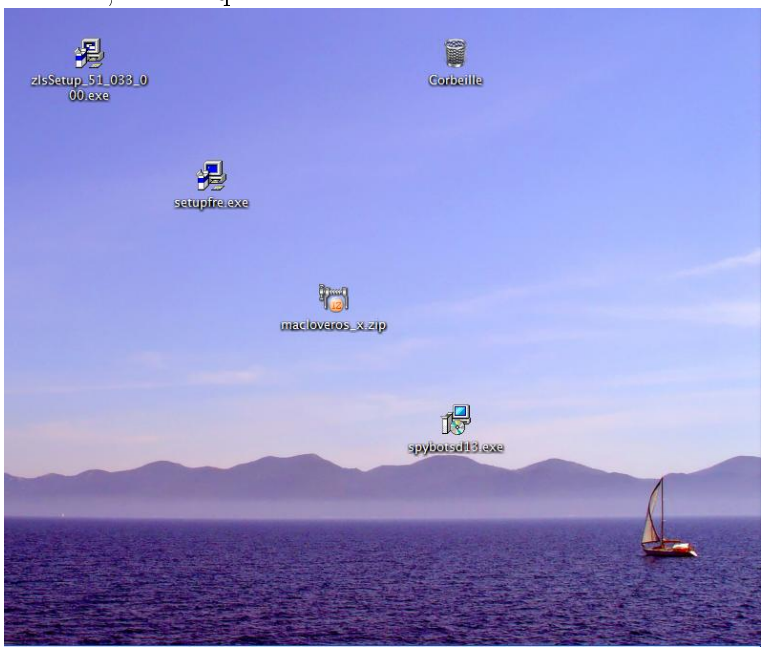
Lorsque vous connectez votre ordinateur à un réseau, il communique avec d'autres ordinateurs. C'est la fonction première d'un réseau. Il peut arriver, et il arrive malheureusement très souvent, qu'un utilisateur malveillant en profite pour introduire dans votre machine un programme indésirable, tel qu'un virus ou un espion. Certains programmes peuvent enregistrer vos mots de passe pour les fournir à un pirate, par exemple.
Sécuriser son ordinateur ne prend pas beaucoup de temps et est un remède très efficace contre toutes les attaques venant de l'extérieur.
Ce document vous permettra de sécuriser Windows[1]. Il n'offre aucune garantie. Néanmoins, j'espère qu'il vous rendra de grands services. A vous de tester !
Les logiciels proposés ici pour sécuriser votre ordinateur sont **entièrement gratuits**. Rien n'est illégal.

2 Comment sécuriser mon ordinateur ?

C'est justement le but de ce document ! Avant de commencer, connectez-vous à Internet, et cliquez sur les liens suivants pour copier les fichiers correspondant sur votre bureau :

- Le programme pare-feu
- Le programme anti-virus préférable à beaucoup de logiciels payants
- Le programme ani-espions
- Un supplément d'ergonomie pour l'anti-virus (*facultatif*)

Au final, voici à quoi devrait ressembler votre bureau :



[1] La procédure ici décrite semble marcher avec Windows XP, et je pense qu'il marchera également avec Windows 98, 2000, Me.

2.1 Enregistrer l'antivirus

Maintenant, il faudra que vous alliez sur la page suivante pour enregistrer cet antivirus. Soyez honnête, vous pouvez donner vos véritables coordonnées, jamais je n'ai reçu de publicité.[2] Il vous permet d'obtenir une licence de l'antivirus valable 14 mois, gratuite et renouvelable gratuitement.

Nous allons maintenant rentrer dans le vif du sujet. Vous êtes prêt(e) ?

2.2 Précaution pas toujours inutile

Je vous conseille de sauver les 4 fichiers téléchargés ainsi que ce document PDF sur un support comme un CD ou un DVD. Si jamais vous êtes amené à réinitialiser votre ordinateur, cette procédure est la première chose à faire après la réinstallation. D'autre part, si vous le pouvez et que votre ordinateur est depuis un certain temps sans protection, je ne saurais que trop vous conseiller de sauvegarder tous vos documents, carnets d'adresses, favoris, sauvegardes et de repartir à zéro, car il y a des chances très grandes pour que votre ordinateur soit déjà atteint par la vermine, pour ne pas dire que c'est certain. En moyenne, il suffit de 5 minutes sans protection pour être touché.

2.3 Première étape : installer le Pare-feu

Voici le programme principal pour protéger votre ordinateur. Avec ça, c'est déjà beaucoup de soucis en moins. Il vous demandera un minimum de patience, mais il n'est pas gênant. Il s'agit de ZoneAlarm. Son rôle est de vous rendre invisible sur Internet, et de contrôler les communications qui arrivent et partent de votre ordinateur. S'il s'aperçoit que le tout nouveau logiciel de retouche photo que vous venez de télécharger souhaite aller sur Internet, il vous demandera s'il faut autoriser. Par principe, il ne faut autoriser un programme à dialoguer avec d'autres ordinateurs que si cela vous semble logique. Pour envoyer et recevoir des e-mails, c'est normal. Pour dessiner, non.
Trêve de longs discours : installons ZoneAlarm.

- Première chose à faire : **Déconnectez-vous d'Internet**. Dans le cas où vous venez de réinitialiser votre ordinateur et où vous avez les fichiers d'installation sur CD, surtout **réalisez cette étape avant de vous connecter à Internet**. Cela diminue très fortement les risques.
- Double-cliquez sur l'icône zlsSetup_51_033_000.exe.

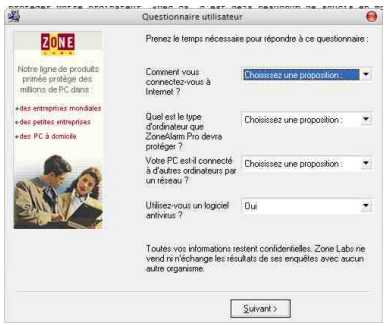
⟶ cliquez sur Suivant.

[2] Si jamais vous craignez les courriers électroniques indésirables, vous pouvez allez visiter Spamgourmet.com qui vous propose des adresses e-mail jetables. Mais dans tous les cas, procédez à l'enregistrement.

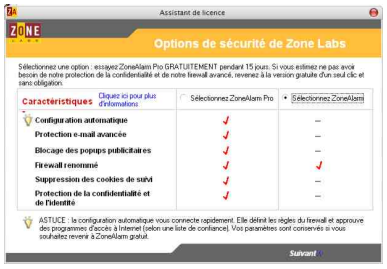
⟶ remplissez les champs demandés avec honnêteté, décochez la première case si vous ne voulez pas être embêté, et cliquez sur Suivant.

⟶ lisez le contrat de licence, cochez la case si vous êtes d'accord, et cliquez sur Suivant si vous avez coché.

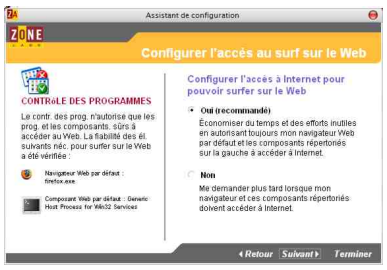
Le programme s'installe et se configure automatiquement.



⟶ A la quatrième question, répondez Oui. Pour les trois premières, cela dépend de votre configuration, vous saurez mieux répondre que moi.
On vous demandera si vous désirez démarrer le programme immédiatement, répondez Oui.

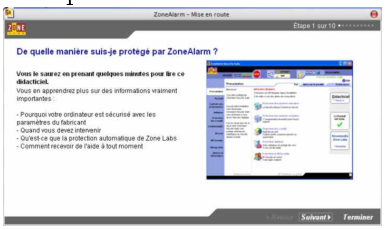


⟶ Répondez : Sélectionnez ZoneAlarm, et cliquez sur Suivant. Puis, cliquez sur terminer. Une nouvelle fenêtre appelée Assistant de configuration s'ouvre : cliquez sur Suivant.

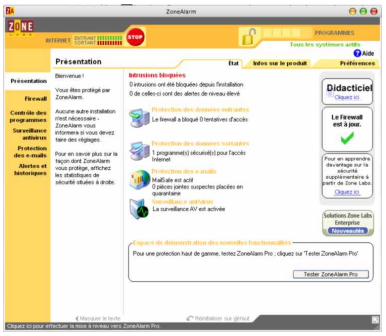


⟶ Vérifiez que Oui est sélectionné, et cliquez sur Suivant, puis sur Terminer

Le programme redémarre alors.
Lorsque l'ordinateur aura redémarré, un didacticiel se mettra en route :



⟶ prenez le temps de le lire, en cliquant à chaque fois sur Suivant, puis en cliquant sur Terminer à la fin. La fenêtre du logiciel s'ouvre alors.

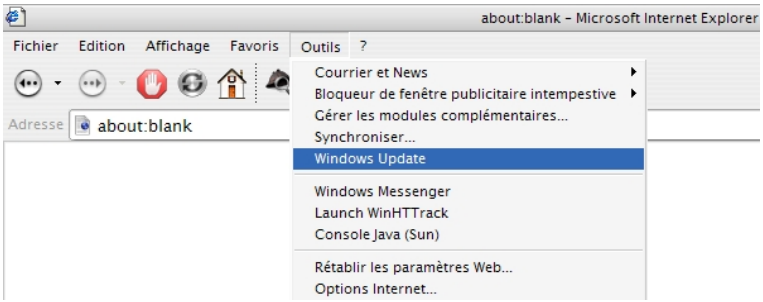


⟶ Vous pouvez cliquer sur la croix, en haut à droite, pour fermer (là où sur ma capture d'écran il n'y a qu'un cercle rouge !)
Un message vous prévient que ceci n'arrête pas la protection de votre ordinateur, cochez la case et cliquez sur OK. **C'est bon !** Votre pare-feu est installé. **Vous pouvez vous reconnecter à Internet**. Au fur et à mesure de l'utilisation, vous recevrez des alertes de ce type :

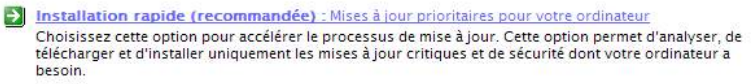
⟶ La première alerte est une constatation : le pare-feu a empêché un ordinateur distant de se connecter au vôtre. Le deuxième vous demande si le logiciel de connexion à Internet a le droit de dialoguer avec un autre ordinateur : répondez que vous Acceptez. Ce sont des exemples. Lorsque vous lancerez votre logiciel de mail, une alerte similaire s'affichera : dites que vous ne voulez plus qu'on vous repose la question, et que vous acceptez. C'est à vous de jouer, maintenant.

2.4 Deuxième étape : Mise à jour de Windows

La deuxième étape de ce processus est de mettre votre version de Windows à jour. Si vous avez une connexion classique que vous payez à la durée, ce processus peut être long. Mais cette étape permet de corriger beaucoup de failles de sécurité de Windows.
Ouvrez Internet Explorer. Cliquez sur Outils puis sur Windows Update. Illustration :



Si vous ne savez pas comment faire, même malgré cela, essayez de cliquer sur ce lien.
Des alertes de sécurité risquent de s'afficher. Vous pouvez a priori faire confiance à Microsoft et autoriser l'installation de quelques logiciels sur votre ordinateur. Ensuite, sélectionnez l'option :



Vous serez guidé pour installer des mises à jour. Il faut toutes les installer, sauf éventuellement le Service Pack 2 de Windows XP (vous pouvez regarder la description). Une fois installées, votre ordinateur sera peut-être amené à redémarrer. **Dans tous les cas, une fois une installation terminée, recommencez cette étape jusqu'à ce qu'il ne reste plus de mise à jour prioritaire autre que le Service Pack 2**.

2.5 Troisième étape : Installation de l'Antivirus

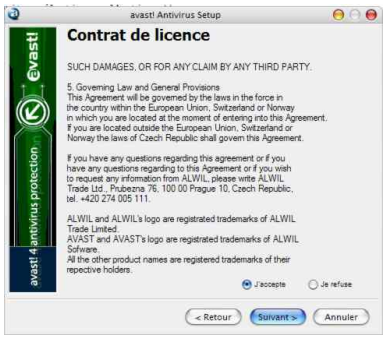
L'antivirus proposé ici est gratuit pour les particuliers ; il se met à jour automatiquement, plusieurs fois par semaine. Il assure également la protection du courrier électronique, de logiciels de partage de fichiers (du type Kazaa). Il surveille la messagerie instantanée. Il est assez complet. Vous avez déjà enregistré cet anti-virus à la partie 3.1 de ce document. Allez consulter vos e-mails. Vous en avez un qui contient :

```
Dear customer,
You were successfully registered for using avast! 4 Home Edition antivirus program.
If you have installed older version (AVAST32), be so kind and download and install
the current version avast! 4 Home Edition (see below).

Your license key is

----- cut here -----
XXXXXXXXXXXXXXXXX-XXXXXXXX
----- cut here -----

The key is valid for home, personal and non-commercial use on Windows workstation
operating systems only!
```

Notez bien la clé (c'est à dire le code noté XXX... ci-dessus) et conservez-le ; si jamais vous deviez réinstaller l'anti-virus, il est toujours mieux de l'avoir sous la main.

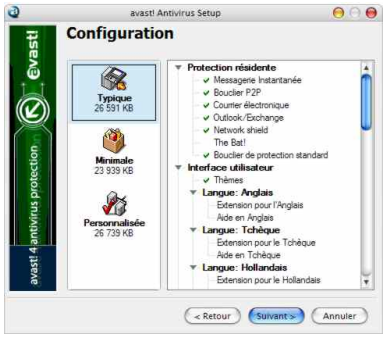
Double-cliquez sur l'icône setupfre.exe.

⟶ Cliquez sur Suivant deux fois.



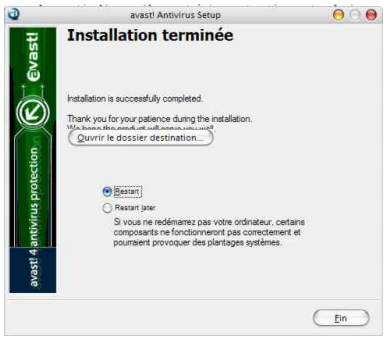
⟶ Lisez le contrat (pour le faire défiler, cliquez sur le texte puis appuyez sur les touches fléchées de votre clavier ↑ et ↓). Cliquez sur J'accepte et sur Suivant.

⟶ Vous pouvez vous créer un dossier. Si vous ne savez pas, laissez tel quel. Puis, cliquez sur Suivant.



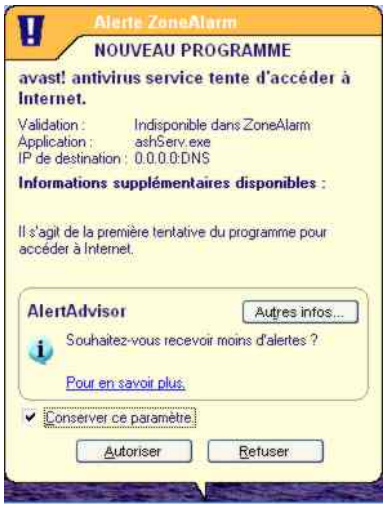
⟶ Sélectionnez l'installation typique et cliquez sur Suivant deux fois.

⟶ Répondez plutôt Non (nous effectuerons cela plus tard).



⟶ Vérifiez que Restart est sélectionné, et cliquez sur Fin. L'ordinateur redémarre.

⟶ Cliquez sur OK.



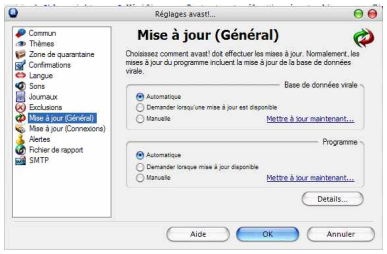
⟶ Il se peut que vous voyiez cette fenêtre : voici un exemple d'alerte ZoneAlarm. L'antivirus cherche à se mettre à jour : cochez la case et cliquez sur Accepter. Normalement, peu de temps après, une douce voix féminine vous informera que la base de données des virus a été mise à jour !

2.6 Quatrième étape : Configuration de l'Antivirus

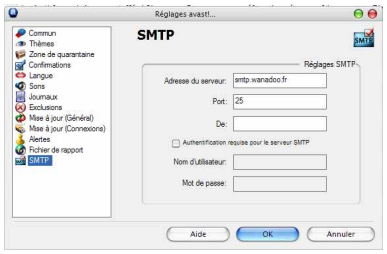
Nous allons tout d'abord activer l'anti-virus : Il faut que vous repériez les deux icônes suivantes sur votre écran : . Cliquez avec le bouton droit de votre souris sur , puis sur A propos d'avast !...

⟶ Cliquez sur Clé de licence..., ici surligné en bleu. Rentrez votre clé, il n'est pas nécessaire de taper le tiret au milieu. Cliquez sur OK et fermez la première fenêtre en cliquant sur OK également.
Maintenant, vous allez mettre le programme et la base de données virale à jour : cliquez avec le bouton droit de votre souris sur , sur Mise à jour, Mise à jour de la base virale. Recommencez avec Mise à jour du programme.
Votre antivirus est maintenant à jour, il faut également lui fournir les informations nécessaires pour qu'il soit efficace.
L'icône symbolise une tâche de l'Antivirus qui crée une base de données (VRDB) vous permettant de sauver 3 versions de chaque fichier exécutable sur votre ordinateur. Cette base de données est conseillée, néanmoins, elle prend beaucoup de place sur le disque dur. En cliquant avec le bouton droit sur l'icône, vous pouvez choisir de ne pas la créer en cliquant sur Invalider la

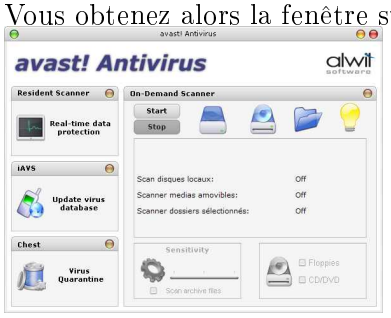
génération de la VRDB, ou choisir à quel moment il doit la créer. Enfin, si l'icône vous embête, cliquez avec le bouton droit dessus et cliquez sur Fusionner avec l'icône principale d'avast !. Vous n'aurez plus que l'icône et en cliquant dessus avec le bouton droit, le sous-menu VRDB vous donnera accès aux mêmes options.
Cliquez maintenant avec le bouton droit sur , et sur Réglages du Programme...



⟶ Dans la partie Mise à jour (Général), je vous conseille de choisir Automatique pour la mise à jour du programme.



⟶ D'autre part dans l'onglet SMTP, tapez l'adresse du serveur SMTP que vous utilisez pour envoyer du courrier électronique[3].
Maintenant, on va rendre l'Antivirus agréable à utiliser : Double-cliquez sur l'icône macloveros_x.zip sur votre bureau, extrayez les fichiers et double-cliquez sur MacLoverOSX.aswcs ; l'antivirus se lance avec une interface simple à appréhender, mais c'est une question de choix personnels.
Maintenant, on va apprendre à utiliser l'antivirus, je vous conseille d'analyser assez régulièrement votre ordinateur, tous les deux mois au minimum, plus fréquemment serait mieux. L'analyse peut être assez longue, mais si vous avez des virus, il vaut mieux s'en débarasser, non ?
Cliquez maintenant avec le bouton droit sur , et sur Démarrer avast ! Antivirus. Une autre méthode est de double cliquer sur l'icône Avast ! Antivirus qui s'est installée sur votre bureau. Vous obtenez alors la fenêtre suivante :



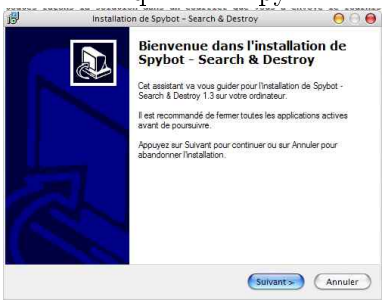
⟶ à droite du bouton Start, quatre icônes symbolisant le disque dur, les médias amovibles, un dossier quelconque et une icône pour avoir de l'aide. Cliquez sur la première de ces icônes : Scan disques locaux va s'activer (vous verrez marqué On juste en dessous.) En bas, vous pouvez régler la sensibilité du scan ; pour un premier scan, il est conseillé de le faire minutieux avec Scan des archives. Puis, cliquez sur Start. Le programme va chercher les virus.
Si votre programme trouve un virus, il vous demandera que faire. Essayez d'abord de réparer le programme. S'il n'y arrive pas, mettez-le en quarantaine : la zone de quarantaine est un endroit de votre disque dur où aucun programme n'aura accès. Le virus sera ainsi isolé, mais le programme ne pourra plus fonctionner. Si jamais le programme ainsi mis en quarantaine est essentiel pour le fonctionnement de votre ordinateur, vous pouvez le replacer en mode normal, mais il sera toujours infecté. Si le programme ne vous manque pas, il sera supprimé au bout d'un

[3]Si vous ne la connaissez pas, entrez, en fonction de votre fournisseur d'accès à Internet, smtp.wanadoo.fr, smtp.free.fr, smtp.tele2.fr... Si vous n'êtes ni client Wanadoo, ni client Free, ni client Tele2, essayez quelque-chose de similaire. Vous devez avoir de toutes façons la solution dans un courrier que vous a envoyé le fournisseur d'accès à votre inscription chez lui, ainsi que dans les propriétés de votre compte e-mail. Pour AOL, ne mettez rien.

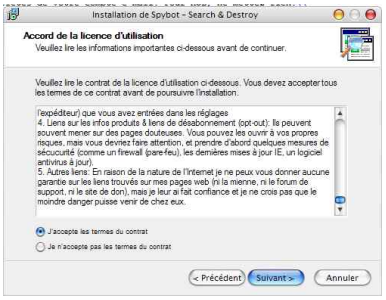
certain temps.

2.7 Dernière étape : installer l'Anti-espions

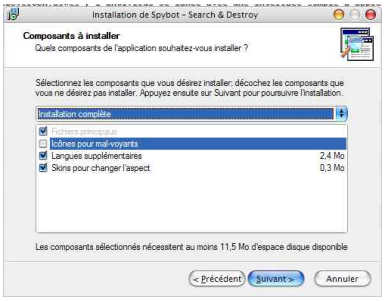
Ce programme n'est pas vraiment un programme pour la sécurité, mais pour la vie privée. Double-cliquez sur spybotsd13.exe sur le bureau. Sélectionnez le français, et cliquez sur OK.



⟶ Cliquez sur Suivant.

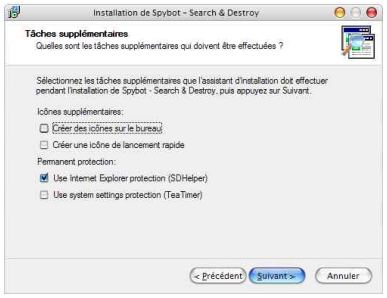


⟶ Lisez le contrat de licence (pour une fois que ça change du discours rébarbatif habituel), cliquez sur J'accepte les termes du contrat, puis sur Suivant.
Encore une fois, vous êtes invités à choisir le dossier d'installation. Si vous ne savez pas, laissez tel quel. Cliquez sur Suivant



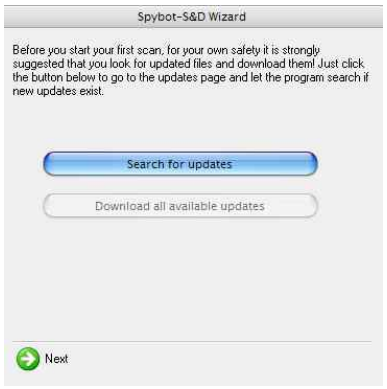
⟶ Dans le menu, sélectionnez Installation complète (si vous êtes mal voyant, installation complète pour mal voyants) et cliquez sur Suivant.

⟶ Si vous ne savez pas quoi faire, cliquez sur Suivant. Sinon, libre à vous de choisir le dossier du menu Démarrer où vous voulez mettre les icônes.



⟶ Laissez tel quel, et cliquez sur Suivant. Si vous vouliez cocher TeaTimer[4], libre à vous de le faire.
Sur l'écran qui suit, cliquez sur Installer. Après l'installation, ne décochez rien et cliquez sur Terminer.

⟶ Cliquez sur Create Registry Backup, patientez, puis cliquez sur Next lorsque le bouton redevient vert.



⟶ Cliquez sur Search for Updates (ici ZoneAlarm va vous demandez si vous autorisez, acceptez), puis s'il y a des mises à jours disponibles, cliquez sur Download all available updates. Puis cliquez sur Next.

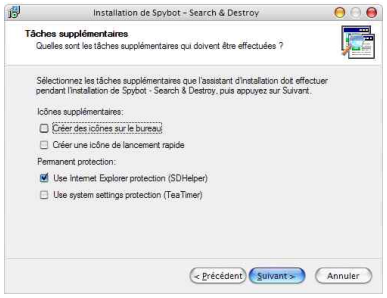
⟶ Cliquez sur Immunize[5] this system, puis sur Next.

Ensuite, vous pouvez choisir de lire le tutoriel, le fichier d'aide, ou bien de commencer à utiliser le logiciel. Cliquez sur Start using the program, à moins que vous ne souhaitiez faire autre

[4] TeaTimer détecte les changements importants qui surviennent dans la base de registre : un programme ajouté au démarrage du système, la page d'accueil de votre navigateur qui est modifiée, etc. Il vous demande de valider ces changements.

[5] il s'agit d'une sorte de vaccination ou protection définitive contre certaines saletés

chose.



⟶ Cliquez sur Vérifier tout. Le balayage commence.

Au final, vous devez vous retrouver avec un écran comme ceci :

⟶ Ici, DSO Exploit est en rouge : il s'agit d'un espion. Si dans la liste vous avez des éléments en vert, ils ne sont pas cochés par défaut : il s'agit juste d'informations stockées sur votre ordinateur qui pourraient intéresser les programmes espions, comme par exemple les derniers titres musicaux que vous avez écoutés, les pages web que vous avez visitées, etc. Les entrées en rouge sont cochées par défaut. Cliquez sur Corriger les problèmes.

⟶ Cliquez sur Oui.

C'est terminé, les espions ont été neutralisés.

3 Annexes

3.1 Maintenance

Maintenant que tous ces programmes ont été installés sur votre ordinateur, je vous conseille de lancer l'antivirus et l'antiespions en même temps, tous les mois ou tous les deux mois. Se débrouiller avec ces logiciels n'est pas tellement difficile.

3.2 Remerciements

Ce document est largement inspiré du site de Sébastien Sauvage. La mise en forme LaTeXdoit beaucoup à Stéphane Barrault, grâce à sa page sur PDFLaTeX. Le Guide LaTeXde l'ENSTA m'a été beaucoup utile également.